

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2002-342168
 (43) Date of publication of application : 29.11.2002

(51) Int.CI.
 G06F 12/14
 G06F 12/00
 G09C 1/00
 H04L 9/08
 H04L 9/10
 H04L 9/32

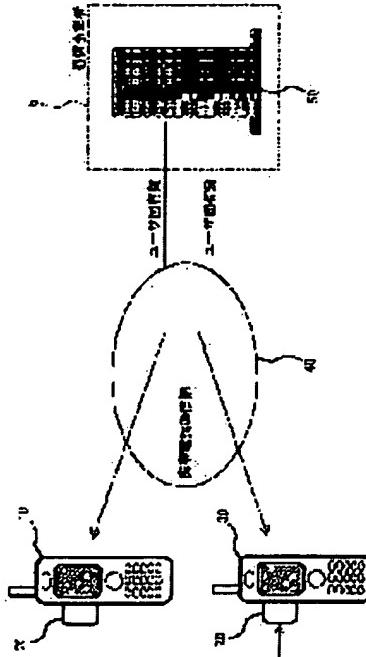
(21) Application number : 2001-144826 (71) Applicant : J-PHONE EAST CO LTD
 (22) Date of filing : 15.05.2001 (72) Inventor : HIGUCHI KAZUHISA
 UETSUKI SHINJI
 FUKAYA MASATO

(54) METHOD FOR MOVING TERMINAL STORAGE DATA BETWEEN INFORMATION COMMUNICATION TERMINALS, INFORMATION PROCESSOR FOR CRYPTOGRAPHIC KEY MANAGEMENT, INFORMATION COMMUNICATION TERMINAL AND PROGRAM

(57) Abstract:

PROBLEM TO BE SOLVED: To make the movement of terminal storage data between portable telephone sets reliable while securing copyright protection to the terminal storage data stored in a portable telephone set.

SOLUTION: The terminal storage data stored in a portable telephone set 10 before exchange are enciphered by using a user-specific key downloaded from a user management server 50, the enciphered terminal storage data are written to a memory card 20, the enciphered terminal storage data written in the memory card 20 are read with an exchanged portable telephone 30, and the terminal storage data read with the exchanged portable telephone 30 are decoded by using the user-specific key downloaded from the user management server 50.



LEGAL STATUS

[Date of request for examination] 26.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-342168

(P2002-342168A)

(43)公開日 平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷

G 0 6 F 12/14
12/00
G 0 9 C 1/00
H 0 4 L 9/08
9/10

識別記号

3 2 0
5 3 7
6 6 0

F I

G 0 6 F 12/14
12/00
G 0 9 C 1/00
H 0 4 L 9/00

テ-マコ-ト*(参考)

3 2 0 B 5 B 0 1 7
5 3 7 H 5 B 0 8 2
6 6 0 D 5 J 1 0 4
6 0 1 B
6 7 1

審査請求 未請求 請求項の数14 O.L (全14頁) 最終頁に統く

(21)出願番号

特願2001-144826(P2001-144826)

(22)出願日

平成13年5月15日(2001.5.15)

(71)出願人 594106346

ジェイフォン東日本株式会社
東京都新宿区信濃町34番地 JR信濃町ビル

(72)発明者 橋口 和久

東京都新宿区信濃町34番地 JR信濃町ビル ジェイフォン東日本株式会社内

(72)発明者 植月 伸次

東京都新宿区信濃町34番地 JR信濃町ビル ジェイフォン東日本株式会社内

(74)代理人 100098626

弁理士 黒田 勇

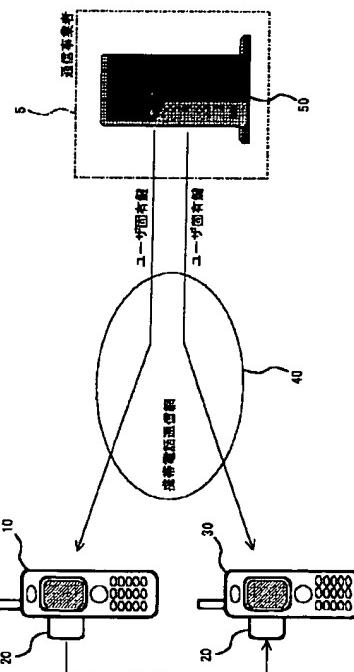
最終頁に統く

(54)【発明の名称】 情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラム

(57)【要約】

【課題】 携帯電話機に保存された端末保存データに対する著作権保護を確保しつつ、携帯電話機間の端末保存データの移動を確実に行う。

【解決手段】 ユーザ管理サーバ50からダウンロードしたユーザ固有鍵を用いて、交換前の携帯電話機10内に保存されている端末保存データを暗号化し、暗号化された端末保存データをメモリーカード20に書き込み、メモリーカード20内に暗号化して書き込んだ端末保存データを交換後の携帯電話機30に読み込み、ユーザ管理サーバ50からダウンロードしたユーザ固有鍵を用いて、交換後の携帯電話機30に読み込んだ端末保存データを復号化する。



【特許請求の範囲】

【請求項1】情報通信端末に保存されている端末保存データを他の情報通信端末に移す情報通信端末間の端末保存データ移動方法であって、
利用者固有の暗号鍵情報を用いて、データ移動元の情報通信端末内に保存されている端末保存データを暗号化するステップと、
該暗号化された端末保存データを記録媒体に書き込むステップと、
該記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込むステップと、
利用者固有の暗号鍵情報を用いて、該データ移動先の情報通信端末に読み込んだ該端末保存データを復号化するステップとを実行することを特徴とする情報通信端末間の端末保存データ移動方法。

【請求項2】請求項1の情報通信端末間の端末保存データ移動方法において、
上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に着脱可能な記録媒体に書き込むことを特徴とする情報通信端末間の端末保存データ移動方法。

【請求項3】請求項1の情報通信端末間の端末保存データ移動方法において、
上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末との間で通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込むことを特徴とする情報通信端末間の端末保存データ移動方法。

【請求項4】請求項1、2又は3の情報通信端末間の端末保存データ移動方法において、
上記利用者固有の暗号鍵情報を、暗号鍵管理用情報処理装置から通信回線を介して上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に登録することを特徴とする情報通信端末間の端末保存データ移動方法。

【請求項5】情報通信端末の利用者が該情報通信端末内に保存している端末保存データを暗号化及び復号化するときに用いる利用者固有の暗号鍵情報を管理する暗号鍵管理用情報処理装置であって、

利用者固有の暗号鍵情報を生成する暗号鍵情報生成手段と、
該利用者固有の暗号鍵情報と利用者の情報を関連づけて記憶する利用者情報記憶手段と、

該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報を、通信回線を介して該利用者の情報通信端末に送信する暗号鍵情報送信手段とを備えたことを特徴とする暗号鍵管理用情報処理装置。

【請求項6】請求項5の暗号鍵管理用情報処理装置において、

上記利用者の情報通信端末から本人確認情報を受信する本人確認情報受信手段と、該本人確認情報に基づいて、該情報通信端末を操作している利用者が本人であるかどうかを確認する本人確認手段とを備え、

上記暗号鍵情報送信手段を、該利用者が本人であることを確認したときに、上記利用者固有の暗号鍵情報を通信回線を介して該利用者の情報通信端末に送信するように構成したことを特徴とする暗号鍵管理用情報処理装置。

【請求項7】請求項5又は6の暗号鍵管理用情報処理装置に用いるコンピュータで実行するプログラムであつて、

該コンピュータを、該暗号鍵管理用情報処理装置における各手段の少なくとも一つとして機能させるためのプログラム。

【請求項8】端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であつて、

利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、

該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、

該暗号化された端末保存データを該記録媒体に書き込むデータ書き手段とを備えたことを特徴とする情報通信端末。

【請求項9】端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であつて、

利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、

該利用者固有の暗号鍵情報を用いて、該記録媒体に記録されている暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とする情報通信端末。

【請求項10】端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であつて、

利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、

該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、

該暗号化された端末保存データを、通信回線を介して端末保存データ管理用情報処理装置に送信する端末保存データ送信手段とを備えたことを特徴とする情報通信端末。

【請求項11】端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であつて、

利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、

端末保存データ管理装置から通信回線を介して、暗号化された端末保存データを受信する端末保存データ受信手段と、

該利用者固有の暗号鍵情報を用いて、該暗号化された端

末保存データを復号化する復号化手段とを備えたことを特徴とする情報通信端末。

【請求項12】請求項8、9、10又は11の情報通信端末において、暗号鍵管理用情報処理装置から送信されてきた上記利用者固有の暗号鍵情報を、通信回線を介して受信する暗号鍵情報受信手段を備えたことを特徴とする情報通信端末。

【請求項13】請求項12の情報通信端末において、通信回線を介して暗号鍵管理用情報処理装置に本人確認情報を送信する本人確認情報送信手段を備えたことを特徴とする情報通信端末。

【請求項14】請求項8、9、10、11、12又は13の情報通信端末に用いるコンピュータで実行するプログラムであって、

該コンピュータを、上記情報通信端末における各手段の少なくとも一つとして機能させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報通信端末の交換等のときに、データ移動元の情報通信端末に保存されている画像データ、音楽データ、プログラムデータ等の端末保存データを、データ移動先の情報通信端末に移すための情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラムに関するものである。

【0002】

【従来の技術】携帯電話機等の情報通信端末では、インターネット上の情報提供サイトや携帯電話通信事業者等が管理運営する情報提供システム等から、画像データ、音声データ、プログラムデータ等をダウンロードして情報通信端末内に保存し、これらのデータを情報通信端末上で表示したり起動したりして利用する場合があった。このようにインターネット等からダウンロードして情報通信端末内に保存した端末保存データの中には、著作権で保護されたものがある。特に、有料でダウンロードされた画像データ、音楽データ、ゲームなどのプログラムデータ等の多くは著作権で保護されたものである。このように著作権で保護された端末保存データは無断で複製したり第三者へ譲渡したりすることができず、基本的にデータをダウンロードした利用者の情報通信端末での使用に制限されている。

【0003】一方、上記携帯電話機等の情報通信端末は、機種変更、故障、不具合発生等により新しい情報通信端末に交換する場合がある。この情報通信端末を交換する際に、上記インターネット等からダウンロードして交換前の情報通信端末に保存している端末保存データを、交換後の新しい情報通信端末でもそのまま使用したいときがある。

【0004】従来、上記情報通信端末を交換するときに

情報端末間で端末保存データを移す方法としては、メモリーカード等の記録媒体を用いた方法が知られている。この方法では、交換前の情報通信端末内に保存されている端末保存データを情報通信端末に装着した記録媒体に書き込み、このデータが書き込まれた記録媒体を新しい交換後の情報通信端末に装着し、記録媒体から交換後の情報通信端末内に端末保存データを読み込む。

【0005】

【発明が解決しようとする課題】ところが、上記従来の情報通信端末間の端末保存データ移動方法では、上記メモリーカード等の記録媒体におけるデータの保護が不十分であったので、端末保存データが著作権で保護されている場合に、第三者への譲渡等を防止して著作権保護を確保しつつ、端末保存データを交換後の情報通信端末に移すことが難しかった。

【0006】なお、上記端末保存データの著作権保護を確保するために、ユニークなID等の暗号鍵情報を用いてデータを暗号化して保存するセキュリティ機能を有するメモリーカード等の記録媒体を用いる方法が考えられる。しかしながら、この方法では、情報通信端末の利用者が端末保存データを第三者に不正に譲渡したり、他の機器に不正に複製したりすることまで防止することは難しいという問題あった。また、上記端末保存データの著作権保護を確保するために、携帯電話番号等の端末識別番号ごとに設定された端末固有の暗号鍵情報で暗号化してデータを受け渡す方法が考えられる。しかしながら、情報通信端末の交換の際に端末識別番号を変えようすると、利用者が同じであっても交換後の情報通信端末上で暗号化された端末保存データを復号化できないという問題があった。

【0007】本発明は以上の問題点に鑑みなされたものであり、その目的は、情報通信端末に保存された端末保存データに対する著作権保護を確保しつつ、情報通信端末間の端末保存データの移動を確実に行うことができる情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラムを提供することである。

【0008】

【課題を解決するための手段】上記目的を達成するためには、請求項1の発明は、情報通信端末に保存されている端末保存データを他の情報通信端末に移す情報通信端末間の端末保存データ移動方法であって、利用者固有の暗号鍵情報を用いて、データ移動元の情報通信端末内に保存されている端末保存データを暗号化するステップと、該暗号化された端末保存データを記録媒体に書き込むステップと、該記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込むステップと、利用者固有の暗号鍵情報を用いて、該データ移動先の情報通信端末に読み込んだ該端末保存データを復号化するステップとを実行することを特徴とするもの

である。

【0009】ここで、上記「情報通信端末」には、PDC (Personal Digital Cellular) 方式、GSM (Global System for Mobile Communication) 方式、TIA (Telecommunications Industry Association) 方式等の携帯電話機、IMT (International Mobile Telecommunications) - 2000で標準化された携帯電話機、PHS (Personal Handyphone Service) 、自動車電話等の電話機のほか、携帯電話モジュールを付加した情報通信端末も含まれる。また、この「情報通信端末」は、上記携帯電話機などの移動型の情報通信端末でいいし、ディスクトップ型パソコン 컴퓨터などの固定型の情報通信端末であってもよい。また、上記「端末保存データ」としては、情報通信端末内に保存されている、画像データ、音楽データ、Javaなどのプログラム言語で記述されたプログラムデータなどが挙げられる。また、上記「利用者固有の暗号鍵情報」は、情報通信端末の使用開始時にその情報通信端末内に登録してもいいし、情報通信端末での暗号化や復号化の際に外部の暗号鍵管理用情報処理装置から通信回線を介して情報通信端末に受信して登録するようにしてもよい。また、上記「利用者固有の暗号鍵情報」の生成は、情報通信端末の使用開始時に行なってもいいし、情報通信端末での暗号化や復号化の際に行ってもよい。

【0010】請求項1の端末保存データ移動方法では、データ移動元の情報通信端末内に保存されている端末保存データを、利用者固有の暗号鍵情報を用いて暗号化して記録媒体に書き込むことにより、第三者が記録媒体からデータを読み出して復号化できないようにする。そして、上記記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込み、上記利用者固有の暗号化鍵情報を用いて復号化することにより、端末保存データをデータ移動先の情報通信端末で使用できるようになる。なお、上記利用者固有の暗号鍵情報はそれぞれ、データ移動元の情報通信端末内及びデータ移動先の情報通信端末内の使用に制限されているものが好ましい。この場合は、利用者固有の暗号鍵情報を他の機器に移して使用できなくなるので、利用者自身が上記記録媒体に書き込まれている端末保存データを他の機器で復号して不正に使用することを防止できる。

【0011】請求項2の発明は、請求項1の情報通信端末間の端末保存データ移動方法において、上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に着脱可能な記録媒体に書き込むことを特徴とするものである。ここで、上記「着脱可能な記録媒体」には、SDメモリーカードのほか、CF (コンパクトフラッシュ (登録商標)) メモリーカード、スマートメディア、メモリースティック、MMC (マルチメディアカード) 等も含まれる。

【0012】請求項2の端末保存データ移動方法では、データ移動元の情報通信端末に装着した記録媒体に上記暗号化された端末保存データを書き込む。そして、この記録媒体をデータ移動先の情報通信端末に装着することにより、記録媒体内の暗号化された端末保存データを読み込んで復号化し、データ移動先の情報通信端末で使用できる。

【0013】請求項3の発明は、請求項1の情報通信端末間の端末保存データ移動方法において、上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末との間で通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込むことを特徴とするものである。

【0014】請求項3の端末保存データ移動方法では、データ移動元の情報通信端末内の暗号化された端末保存データを、通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込む。そして、この情報処理装置から送信された暗号化済みの端末保存データをデータ移動先の情報通信端末で受信して復号化し、データ移動先の情報通信端末で使用できる。

【0015】請求項4の発明は、請求項1、2又は3の情報通信端末間の端末保存データ移動方法において、上記利用者固有の暗号鍵情報を、暗号鍵管理用情報処理装置から通信回線を介して上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に登録することを特徴とするものである。

【0016】請求項4の端末保存データ移動方法では、上記利用者固有の暗号鍵情報が、通信回線を介して暗号鍵管理用情報処理装置から登録できるため、各利用者の情報通信端末で用いる利用者固有の暗号鍵情報を一元管理できるようになる。

【0017】請求項5の発明は、情報通信端末の利用者が該情報通信端末内に保存している端末保存データを暗号化及び復号化するときに用いる利用者固有の暗号鍵情報を管理する暗号鍵管理用情報処理装置であって、利用者固有の暗号鍵情報を生成する暗号鍵情報生成手段と、該利用者固有の暗号鍵情報と利用者の情報とを関連づけて記憶する利用者情報記憶手段と、該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報を、通信回線を介して該利用者の情報通信端末に送信する暗号鍵情報送信手段とを備えたことを特徴とするものである。

【0018】請求項5の暗号鍵管理用情報処理装置では、暗号鍵情報生成手段で利用者固有の暗号鍵情報が生成され、利用者固有の暗号鍵情報と利用者の情報と関連づけられて利用者情報記憶手段に記憶される。そして、暗号鍵情報送信手段により、該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報が、通信回線を介して該利用者の情報通信端末に送信される。暗号鍵管理用情報処理装置から送信された利用者固有の暗号鍵情報は、各利用者の情報通信端末で受信されて登録され、端

末保存データの暗号化及び復号化に用いられる。

【0019】請求項6の発明は、請求項5の暗号鍵管理用情報処理装置において、上記利用者の情報通信端末から本人確認情報を受信する本人確認情報受信手段と、該本人確認情報に基づいて、該情報通信端末を操作している利用者が本人であるかどうかを確認する本人確認手段とを備え、上記暗号鍵情報送信手段を、該利用者が本人であることを確認したときに、上記利用者固有の暗号鍵情報を通信回線を介して該利用者の情報通信端末に送信するように構成したことを特徴とするものである。

【0020】請求項6の暗号鍵管理用情報処理装置では、本人確認情報受信手段で利用者の情報通信端末から本人確認情報が受信され、この本人確認情報に基づいて、本人確認手段により該情報通信端末を操作している利用者が本人であるかどうかが確認される。そして、上記暗号鍵取得要求データを送ってきた利用者が本人であると確認されたときに、上記暗号鍵情報送信手段により、利用者固有の暗号鍵情報が通信回線を介して利用者の情報通信端末に送信される。

【0021】請求項7の発明は、請求項5又は6の暗号鍵管理用情報処理装置に用いるコンピュータで実行するプログラムであって、該コンピュータを、該暗号鍵管理用情報処理装置における各手段の少なくとも一つとして機能させるためのプログラムである。

【0022】請求項7のプログラムを暗号鍵管理用情報処理装置で用いるコンピュータで実行することにより、暗号鍵管理用情報処理装置における各種情報処理を実行することができる。

【0023】請求項8の発明は、端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、該暗号化された端末保存データを該記録媒体に書き込むデータ書き手段とを備えたことを特徴とするものである。

【0024】請求項8の情報通信端末では、端末保存データ記憶手段に記憶されている端末保存データが利用者固有の暗号鍵情報を用いて暗号化されて記録媒体に書き込まれるため、第三者が記録媒体からデータを読み出して復号化できない。

【0025】請求項9の発明は、端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該記録媒体に記録されている暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とするものである。

【0026】請求項9の情報通信端末では、記録媒体内の暗号化された端末保存データが読み出され、利用者固

有の暗号鍵情報を用いて復号化されて使用可能となる。

【0027】請求項10の発明は、端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、該暗号化された端末保存データを、通信回線を介して端末保存データ管理用情報処理装置に送信する端末保存データ送信手段とを備えたことを特徴とするものである。

【0028】請求項10の情報通信端末では、端末保存データ記憶手段に記憶されている端末保存データが利用者固有の暗号鍵情報を用いて暗号化され、通信回線を介して端末保存データ管理用情報処理装置に送信されて管理されるため、第三者がデータを読み出して復号化できない。

【0029】請求項11の発明は、端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、端末保存データ管理装置から通信回線を介して、暗号化された端末保存データを受信する端末保存データ受信手段と、該利用者固有の暗号鍵情報を用いて、該暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とするものである。

【0030】請求項11の情報通信端末では、暗号化された端末保存データが端末保存データ管理装置から通信回線を介して受信され、利用者固有の暗号鍵情報を用いて復号化されて使用可能となる。

【0031】なお、上記請求項8、9、10及び11の情報通信端末で用いる利用者固有の暗号鍵情報はそれぞれ、情報通信端末内での使用に制限された状態で上記暗号化鍵情報記憶手段に記憶するのが好ましい。この場合は、利用者固有の暗号鍵情報を他の機器に移して使用できなくなるので、利用者自身が上記暗号化されている端末保存データを他の機器で復号して不正に使用することを防止できる。

【0032】請求項12の発明は、請求項8、9、10又は11の情報通信端末において、暗号鍵管理用情報処理装置から送信してきた上記利用者固有の暗号鍵情報を、通信回線を介して受信する暗号鍵情報受信手段を備えたことを特徴とするものである。

【0033】請求項12の情報通信端末では、必要に応じて、暗号鍵管理用情報処理装置から送信してきた利用者固有の暗号鍵情報を、通信回線を介して受信し、端末保存データの暗号化や復号化に用いることができる。

【0034】請求項13の発明は、請求項12の情報通信端末において、通信回線を介して暗号鍵管理用情報処理装置に本人確認情報を送信する本人確認情報送信手段を備えたことを特徴とするものである。

【0035】請求項13の情報通信端末では、本人確認情報送信手段で通信回線を介して暗号鍵管理用情報処理

装置に本人確認情報を送信することにより、暗号鍵管理用情報処理装置で利用者の本人確認を行った後、利用者固有の暗号鍵情報を情報通信端末に送信することができるようになる。

【0036】請求項14の発明は、請求項8、9、10、11、12又は13の情報通信端末に用いるコンピュータで実行するプログラムであって、該コンピュータを、上記情報通信端末における各手段の少なくとも一つとして機能させるためのプログラムである。

【0037】請求項14のプログラムを情報処理端末で用いるコンピュータで実行することにより、情報通信端末における各種情報処理を実行することができる。

【0038】なお、上記請求項7又は14の発明に係るプログラムの受け渡しは、デジタル情報としてプログラムを記録したFD、CD-ROM等の記録媒体を用いて行なってもいいし、コンピュータネットワーク等の通信回線を用いて行なってもよい。

【0039】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。

【実施形態1】図1は、本発明の第1の実施形態に係る端末保存データ移動方法の概念図である。本実施形態の端末保存データ移動方法は、情報通信端末としての携帯電話機を機種変更等の理由で交換するときに、データ移動元の携帯電話機（以下「交換前の携帯電話機」という。）からデータ移動先の新しい携帯電話機（以下「交換後の携帯電話機」という。）に、有料でダウンロードした待ち受け画面等の画像データ、着信メロディ等の音楽データ、ゲームソフトなどのJavaプログラムデータなどの著作権で保護されている端末保存データを移す方法である。

【0040】図1において、交換前の携帯電話機10内に保存されている端末保存データは、交換前の携帯電話機10内の使用に制限されている利用者固有の暗号鍵情報（以下、「ユーザ固有鍵」という。）を用いて暗号化され、携帯電話機10に着脱可能な記録媒体としてのメモリーカード20に書き込まれる。上記メモリーカード20は交換後の携帯電話機30に装着され、メモリーカード20内に暗号化して書き込まれた端末保存データが、交換後の携帯電話機30に読み込まれる。交換後の携帯電話機30は、交換後の携帯電話機30での使用に制限されているユーザ固有鍵を用いて復号化される。上記交換前後の携帯電話機10、30で使用されるユーザ固有鍵は、通信回線としての携帯電話通信網40を介して、通信事業者5が管理運営する暗号鍵管理用情報処理装置としてのユーザ管理サーバ50からダウンロードされる。

【0041】図2及び図3はそれぞれ、本端末保存データ移動方法に用いられるユーザ管理サーバ50の概略構成図及び機能ブロック図である。このユーザ管理サーバ

50は通信事業者5によって管理運営され、図2に示すように、システムバス100、CPU101、RAM102やROM103等からなる内部記憶装置、ハードディスクドライブ（HDD）や光ディスクドライブ等からなる外部記憶装置104、マウスやキーボード等からなる入力装置105、ディスプレイやプリンタ等からなる出力装置106、及び携帯電話通信網40を介して各利用者10の携帯電話機60と通信するための携帯電話用通信装置108を備えている。CPU101やRAM102等の構成要素はお互いに、システムバス100を介して、データやプログラムの命令等のやり取りを行っている。この認証システム51を所定の手順に従って動作させるためのプログラムはROM103や外部記憶装置104に記憶されており、必要に応じてCPU101やRAM102上の作業エリアに呼び出されて実行される。また、上記ユーザ管理サーバ50は1台のコンピュータシステムで構成してもいいし、各種データを関連付けて管理するデータベースサーバ等のような複数のサーバ機能をそれぞれ受け持つ複数台のコンピュータをネットワークで結んで構成してもよい。

【0042】ユーザ管理サーバ50は、図2に示したハードウェア上で所定のプログラムを実行することにより、図3に示す利用者情報記憶手段501、暗号鍵情報生成手段502及び暗号鍵情報送信手段503の各機能を実現している。上記利用者情報記憶手段501は、上記ユーザ管理サーバ50のハードディスク等からなる外部記憶装置104を用いて構成されており、携帯電話機10、30を所有している利用者に関する利用者情報と、ユーザ固有鍵とを関連付けて記憶している。この利用者情報は、各利用者について、端末識別情報としての携帯電話番号や、本人確認情報としてのPINコード等が関連付けられて登録されている。

【0043】また、上記ユーザ固有鍵としては、様々な暗号アルゴリズムで使用する暗号鍵を使用することができ、鍵長についても特定の鍵長に制限されるものではない。また、上記ユーザ鍵は、暗号化する側と復号化する側で同じものを使用する共有型の暗号鍵でもいいし、公開鍵と秘密鍵との組み合わせのように暗号化する側と復号化する側で異なるものを使用する暗号鍵であってもよい。

【0044】上記暗号鍵情報生成手段502は、上記ユーザ管理サーバ50のCPU101、RAM102等により構成され、各利用者ごとに異なるユーザ固有鍵を生成する機能を有している。

【0045】上記暗号鍵情報送信手段503は、上記ユーザ管理サーバ50のCPU101、RAM102、携帯電話用通信装置108等により構成され、利用者情報記憶手段501に記憶されているユーザ固有鍵を、携帯電話通信網40を介して各利用者の携帯電話機10、30に送信する機能を有している。

【0046】図4及び図5はそれぞれ、本端末保存データ移動方法に用いられる携帯電話機10、30の概略構成図及び機能ブロック図である。この携帯電話機10、30は、図4に示すように、システムバス200、CPU201、RAM202やROM203等からなる内部記憶装置、マイクや各種入力ボタン等からなる入力装置204、液晶ディスプレイ(LCD)やスピーカ等からなる出力装置205、メモリーカードに対するデータ書き込み及びデータ読み出を行なうメモリーカードドライブ装置206、携帯電話通信網40を介して他の携帯電話機や上記ユーザ管理サーバ50と通信するための携帯電話用通信装置207を備えている。CPU201やRAM202等の構成要素はお互いに、システムバス200を介して、データやプログラムの命令等のやり取りを行なっている。この携帯電話機10、30を所定の手順に従って動作させるためのプログラムはROM203に記憶されており、必要に応じてCPU201やRAM202上の作業エリアに呼び出されて実行される。

【0047】上記メモリーカード20としては例えばSDメモリーカードを使用することができる。また、このSDメモリーカード以外にも、CF(コンパクトフラッシュ)メモリーカード、スマートメディア、メモリースティック、MMC(マルチメディアカード)等を使用することができる。

【0048】本携帯電話機10、30は、図4に示したハードウェア上で所定のプログラムを実行することにより、図5に示す端末保存データ記憶手段601、暗号鍵情報受信手段602、暗号鍵情報記憶手段603、暗号化手段604、データ書き込手段605、データ読み込手段606及び復号化手段607の各機能を実現している。

【0049】上記端末保存データ記憶手段601は、携帯電話機10、30のCPU201、RAM202等により構成され、インターネット上の情報提供サイトや携帯電話通信事業者等が管理運営する情報提供システム等から待ち受け画面等の画像データ、着信メロディ等の音楽データ、ゲームソフトなどのJavaプログラムデータなどの端末保存データを記憶している。

【0050】上記暗号鍵情報受信手段602は、携帯電話機10、30のCPU201、RAM202、携帯電話通信網用通信装置207等により構成され、上記ユーザ管理サーバ50から携帯電話通信網40を介してユーザ固有鍵を受信する機能を有している。

【0051】上記暗号鍵情報記憶手段603は、携帯電話機10、30のCPU201、RAM202等により構成され、上記暗号鍵情報受信手段602で受信したユーザ固有鍵を、携帯電話機内で使用に限定した状態で記憶する機能を有している。

【0052】上記暗号化手段604は、携帯電話機10、30のCPU201、RAM202等により構成され、上記暗号鍵情報記憶手段603に記憶されているユ

ーザ固有鍵を用いて、上記端末保存データ記憶手段601に記憶されている端末保存データを所定の暗号アルゴリズムにより暗号化する機能を有している。

【0053】上記データ書き込手段605は、携帯電話機10、30のCPU201、メモリーカードドライブ装置206等により構成され、上記暗号化手段604で暗号化された端末保存データを、携帯電話機に装着されたメモリーカード20に書き込む機能を有している。

【0054】上記データ読み込手段606は、携帯電話機10、30のCPU201、メモリーカードドライブ装置206等により構成され、携帯電話機に装着されたメモリーカード20内に保存されている暗号化済みの端末保存データを、携帯電話機10、30内に読み込む機能を有している。

【0055】上記復号化手段607は、携帯電話機10、30のCPU201、RAM202等により構成され、上記暗号鍵情報記憶手段603に記憶されているユーザ固有鍵を用いて、上記データ読み込手段606でメモリーカード20から読み込んだ暗号化済みの端末保存データを所定のアルゴリズムで復号化する機能を有している。復号化された端末保存データは、上記端末保存データ記憶手段601に記憶され、利用者の操作により液晶ディスプレイ(LCD)上に表示したりスピーカから出力したりすることができる。

【0056】図6は、本実施形態の端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャートである。図6中の細い実線で囲まれたステップは交換前の携帯電話機10での処理であり、太い実線で囲まれたステップはユーザ管理サーバ50での処理である。また、図6中の破線で囲まれたステップは、交換後の携帯電話機30での処理である。

【0057】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機10から携帯電話通信網40を介してユーザ管理サーバ50に送信される(ステップ1)。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、交換前の携帯電話機10の利用者に対するユーザ固有鍵が生成され、携帯電話通信網40を介して交換前の携帯電話機10に送信される(ステップ2)。上記ユーザ固有鍵を受信した交換前の携帯電話機10では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される(ステップ3)。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、交換前の携帯電話機10に装着したメモリーカード20に書き込まれる(ステップ4、5)。次に、交換前の携帯電話機10からメモリーカード20が取り外された後、交換後の新しい携帯電話機30に装着され、メモリーカード20内の暗号化済みの端末保存データが交換後の携帯電話機30に読み込まれる(ステップ6)。そして、このデータ読み込みとともに、ユーザ固有鍵をダウンロードするためのユ

ユーザ固有鍵要求データが、交換後の携帯電話機30から携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ7）。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、上記交換前の携帯電話機10に対して送信したものと同じユーザ固有鍵が、携帯電話通信網40を介して交換後の携帯電話機30に送信される（ステップ8）。上記ユーザ管理サーバ50から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機30では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される（ステップ9）。そして、上記メモリーカード20から読み込まれた暗号化済みの端末保存データが、暗号鍵情報記憶手段603に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段601に保存され、利用者が使用できる状態になる（ステップ10）。

【0058】図7は、本実施形態の端末保存データ移動方法における他のデータ移動手順の流れを示すフローチャートである。上記図6の場合と同様に、図7中の細い実線で囲まれたステップは交換前の携帯電話機10での処理であり、太い実線で囲まれたステップはユーザ管理サーバ50での処理である。また、図7中の破線で囲まれたステップは、交換後の携帯電話機30での処理である。

【0059】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機10から携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ1）。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、交換前の携帯電話機10の利用者に対するユーザ固有鍵が生成され、携帯電話通信網40を介して交換前の携帯電話機10に送信される（ステップ2）。上記ユーザ固有鍵を受信した交換前の携帯電話機10では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される（ステップ3）。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、交換前の携帯電話機10に装着したメモリーカード20に書き込まれる（ステップ4、5）。次に、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換後の携帯電話機30から携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ6）。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、上記交換前の携帯電話機10に対して送信したものと同じユーザ固有鍵が、携帯電話通信網40を介して交換後の携帯電話機30に送信される（ステップ7）。そして、上記ユーザ管理サーバ50から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機30では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される（ステップ8）。次に、交換前の携帯電話機10からメモリーカード20が取り外された後、交換後の新しい携帯電話機30に装着され、メモリーカード20内の暗号化済み

の端末保存データが交換後の携帯電話機30に読み込まれる（ステップ9）。そして、このメモリーカード20から読み込まれた暗号化済みの端末保存データが、暗号鍵情報記憶手段603に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段601に保存され、利用者が使用できる状態になる（ステップ10）。

【0060】なお、上記図6及び図7の例では、ユーザ管理サーバ50においてユーザの携帯電話機10からユーザ固有鍵要求データを受信したタイミングでユーザ固有鍵を生成しているが、ユーザ固有鍵は、各ユーザの携帯電話機にダウンロードして利用できる任意のタイミングで生成することができる。例えば、ユーザによる携帯電話機の使用開始にあたって利用者情報をユーザ管理サーバ50に登録する際に、ユーザ管理サーバ50内でそのユーザに対応するユーザ固有鍵を予め生成して記憶しておくようにしてもよい。この場合は、ユーザ固有鍵要求データを送信してからユーザ固有鍵をダウンロードするまでの時間が短くなるので、データ移動作業の効率化を図ることができる。

【0061】以上、本実施形態によれば、携帯電話機10、30内の使用に制限されているユーザ固有鍵を用いて暗号化し、端末保存データを携帯電話機10、30間で移動させることができる。従って、携帯電話機に保存された端末保存データが、有料サイトなどからダウンロードした画像データ、音楽データ、Javaプログラムデータ等の著作権で保護されている場合であっても、これらの端末保存データに対する著作権保護を確保しつつ、携帯電話機の交換時における端末保存データの移動を確実に行うことができる。

【0062】【実施形態2】図8は、本発明の第2の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図である。以下、前述の第1の実施形態の端末保存データ移動方法と同様な部分については、同じ符号を付して説明を省略する。本実施形態の端末保存データ移動方法では、交換前の携帯電話機10で暗号化した端末保存データをメモリーカードに書き込む代わりに、携帯電話通信網40を介してユーザ管理サーバ50に送信して保存し、交換後の携帯電話機30では、携帯電話通信網40を介してユーザ管理サーバ50から暗号化済みの端末保存データを読み込んでいる。

【0063】図9は、本端末保存データ移動方法に用いられるユーザ管理サーバ50の機能ブロック図である。なお、このユーザ管理サーバ50のハードウェア構成としては、上記第1の実施形態で示した図2の構成と同様のものを用いることができる。本ユーザ管理サーバ50は、図2に示したハードウェア上で所定のプログラムを実行することにより、第1の実施形態における利用者情報記憶手段501、暗号鍵情報生成手段502及び暗号鍵情報送信手段503の各機能のほか、端末保存データ

受信手段504、端末保存データ記憶手段505及び端末保存データ送信手段506の各機能を実現している。

【0064】上記端末保存データ受信手段504は、上記ユーザ管理サーバ50のCPU101、RAM102、携帯電話用通信装置108等により構成され、交換前の携帯電話機10から携帯電話通信網40を介して送信されてきた暗号化済みの端末保存データを受信する機能を有している。上記端末保存データ記憶手段505は、上記ユーザ管理サーバ50のCPU101、RAM102等により構成され、交換前の携帯電話機10から受信した暗号化済みの端末保存データを記憶する機能を有している。上記端末保存データ送信手段506は、上記ユーザ管理サーバ50のCPU101、RAM102、携帯電話用通信装置108等により構成され、交換後の携帯電話機30からのダウンロード要求に基づいて、携帯電話通信網40を介して交換後の携帯電話機30に暗号化済みの端末保存データを送信する機能を有している。

【0065】図10は、本端末保存データ移動方法に用いられる携帯電話機10、30の機能プロック図である。なお、この携帯電話機10、30のハードウェア構成としては、メモリーカードドライブ装置206が必須でない点を除いて、上記第1の実施形態で示した図4の構成と同様なものを用いることができる。本携帯電話機10、30は、図4に示したハードウェア上で所定のプログラムを実行することにより、第1の実施形態における端末保存データ記憶手段601、暗号鍵情報受信手段602、暗号鍵情報記憶手段603、暗号化手段604及び復号化手段607のほか、端末保存データ送信手段608及び端末保存データ受信手段609の各機能を実現している。

【0066】上記端末保存データ送信手段608は、上記携帯電話機10、30のCPU201、RAM202、携帯電話通信網用通信装置207等により構成され、携帯電話通信網40を介して上記ユーザ管理サーバ50に暗号化済みの端末保存データを送信する機能を有している。上記端末保存データ受信手段609は、上記携帯電話機10、30のCPU201、RAM202、携帯電話通信網用通信装置207等により構成され、上記ユーザ管理サーバ50から携帯電話通信網40を介して送信されてきた暗号化済みの端末保存データを受信する機能を有している。

【0067】図11は、本実施形態の端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャートである。上記図6及び図7の場合と同様に、図11中の細い実線で囲まれたステップは交換前の携帯電話機10での処理であり、太い実線で囲まれたステップはユーザ管理サーバ50での処理である。また、図11中の破線で囲まれたステップは、交換後の携帯電話機30での処理である。

【0068】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機10から携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ1）。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、交換前の携帯電話機10の利用者に対するユーザ固有鍵が生成され、携帯電話通信網40を介して交換前の携帯電話機10に送信される（ステップ2）。上記ユーザ固有鍵を受信した交換前の携帯電話機10では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される（ステップ3）。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ4、5）。次に、ユーザ管理サーバ50では、交換前の携帯電話機10から送信されてきた暗号化済みの端末保存データが受信され、端末保存データ記憶手段505に保存される（ステップ6）。そして、交換後の携帯電話機30からユーザ管理サーバ50に端末保存データ要求データが送信されると（ステップ7）、ユーザ管理サーバ50では、その利用者に対応した暗号化済みの端末保存データが携帯電話通信網40を介して交換後の携帯電話機30に送信される（ステップ8）。次に、交換後の新しい携帯電話機30では、上記ユーザ管理サーバ50から送信されてきた暗号化済みの端末保存データを受信し（ステップ9）、この受信とともに、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換後の携帯電話機30から携帯電話通信網40を介してユーザ管理サーバ50に送信される（ステップ10）。ユーザ固有鍵要求データを受信したユーザ管理サーバ50では、上記交換前の携帯電話機10に対して送信したものと同じユーザ固有鍵が、携帯電話通信網40を介して交換後の携帯電話機30に送信される（ステップ11）。上記ユーザ管理サーバ50から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機30では、受信したユーザ固有鍵が暗号鍵情報記憶手段603に一旦保存される（ステップ12）。そして、上記ユーザ管理サーバ50から受信した暗号化済みの端末保存データが、暗号鍵情報記憶手段603に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段601に保存され、利用者が使用できる状態になる（ステップ13）。

【0069】なお、上記図11の例においても、前述の図6及び図7の場合と同様に、ユーザ管理サーバ50においてユーザの携帯電話機10からユーザ固有鍵要求データを受信したタイミングでユーザ固有鍵を生成しているが、ユーザ固有鍵は、各ユーザの携帯電話機にダウンロードして利用できる任意のタイミングで生成することができる。例えば、ユーザによる携帯電話機の使用開始にあたって利用者情報をユーザ管理サーバ50に登録する際に、ユーザ管理サーバ50内でそのユーザに対応す

るユーザ固有鍵を予め生成して記憶しておくようにしてもよい。この場合は、ユーザ固有鍵要求データを送信してからユーザ固有鍵をダウンロードするまでの時間が短くなるので、データ移動作業の効率化を図ることができる。

【0070】以上、本実施形態においても、携帯電話機10、30内での使用に制限されているユーザ固有鍵を用いて暗号化し、端末保存データを携帯電話機10、30間で移動させることができる。従って、携帯電話機に保存された端末保存データが、有料サイトなどからダウンロードした画像データ・音楽データ・Javaプログラムデータ等の著作権で保護されている場合であっても、これらの端末保存データに対する著作権保護を確保しつつ、携帯電話機の交換時における端末保存データの移動を確実に行うことができる。特に、本実施形態では、交換前後の携帯電話機の少なくとも一方がメモリーカードを使用できない場合でも、端末保存データを確実に移動させることができる。

【0071】なお、上記第2の実施形態では、ユーザ固有鍵を管理する機能と携帯電話機から送られてきた暗号化済みの端末保存データを管理する機能を、1台のユーザ管理サーバ50に持たせるようにしているが、各機能を別々のサーバで実現するように構成してもよい。また、上記第2の実施形態では、交換後の携帯電話機30において、暗号化済みの端末保存データをダウンロードした後、ユーザ固有鍵をダウンロードしているが、各ダウンロードのタイミングはこれに限定されるものではなく、例えば、暗号化済みの端末保存データに先立ってユーザ固有鍵を予めダウンロードしておいてもよい。

【0072】また、上記各実施形態において、利用者の携帯電話機10、30からユーザ管理サーバ50にユーザ固有鍵要求データを送信するときに、セキュリティを高めるために、本人確認情報としてのPIN(Personal Identification Number)コードも送信し、ユーザ管理サーバ50側で本人確認を行なった後、その利用者に対応したユーザ固有鍵を携帯電話機10、30に送信するようにもよい。この本人確認情報としては、上記PINコードのほか、利用者の指紋情報、眼球の虹彩情報や網膜情報、手等の表面から読みとった血管情報、顔の形、音声の特徴や声紋、手形や掌紋等のバイオメトリクス(生物学的な特徴)に関する情報を用いることができる。また、文字の書き方や筆圧、筆を離す方向などの情報や、キーボードなどから入力するときのスピード等の筆跡情報や、キーと別なキーとを押す間の間隔等の打鍵情報などを用いてもよい。

【0073】また、上記各実施形態では、ユーザ固有鍵をユーザ管理サーバ50からダウンロードして携帯電話機内での暗号化や復号化に使用しているが、利用者による携帯電話機の使用開始時に、携帯電話機内に搭載されているメモリーに保存するようにしてよい。この場合、

セキュリティを高めて著作権保護を確保するために、指紋モジュールや、次世代移動通信システム用のSIMカードであるUSIM(Universal Subscriber Identity Module)のようなセキュアメモリーに、ユーザ固有鍵を保存するのが好ましい。

【0074】また、上記各実施形態では、情報通信端末が携帯電話機の場合について説明したが、本発明は、PHS、自動車電話、携帯型のパソコンなどの他の移動情報端末のほか、固定型のディスクトップパソコンの場合についても適用でき、同様な効果が得られるものである。

【0075】

【発明の効果】請求項1乃至14の発明によれば、利用者固有の暗号鍵情報を用いて暗号化し、端末保存データを情報通信端末間で移動させることができるので、情報通信端末に保存された端末保存データが著作権で保護されている場合であっても、端末保存データに対する著作権保護を確保しつつ、情報通信端末間の端末保存データの移動を確実に行うことができるという優れた効果がある。

【0076】特に、請求項2の発明によれば、情報通信端末に着脱可能な記録媒体を用いることにより、情報通信端末間の端末保存データの移動が簡易になるという優れた効果がある。

【0077】特に、請求項3の発明によれば、情報通信端末が端末保存データ移動のための記録媒体を装着できる機能を有しない場合でも、情報通信端末間の端末保存データの移動が可能になるという優れた効果がある。

【0078】特に、請求項4の発明によれば、各利用者の情報通信端末で用いる利用者固有の暗号鍵情報を一元管理できるようになるという優れた効果がある。

【0079】特に、請求項6の発明によれば、利用者の本人確認を行った後、利用者固有の暗号鍵情報を送信するようになっているので、本人以外の第三者が端末保存データを利用者固有の暗号鍵情報を用いて不正に暗号化したり復号化したりするのを回避することができるという優れた効果がある。

【0080】特に、請求項12の発明によれば、情報通信端末に予め利用者固有の暗号鍵情報が保存されていない場合でも、必要に応じて利用者固有の暗号鍵情報を通信回線を介して取得し、端末保存データの暗号化や復号化に用いることができるという優れた効果がある。

【0081】特に、請求項13の発明によれば、暗号鍵管理用情報処理装置で利用者の本人確認を行った後、利用者固有の暗号鍵情報を情報通信端末に送信することができるので、本人以外の第三者が端末保存データを利用者固有の暗号鍵情報を用いて不正に暗号化したり復号化したりするのを回避することができるという優れた効果がある。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図。

【図2】同端末保存データ移動方法に用いられるユーザ管理サーバの概略構成図。

【図3】同ユーザ管理サーバの機能ブロック図。

【図4】同端末保存データ移動方法に用いられる携帯電話機の概略構成図。

【図5】同携帯電話機の機能ブロック図。

【図6】同端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャート。

【図7】変形例に係るデータ移動手順の流れを示すフローチャート。

【図8】本発明の第2の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図。

【図9】同端末保存データ移動方法に用いられるユーザ管理サーバの機能ブロック図。

【図10】同端末保存データ移動方法に用いられる携帯電話機の機能ブロック図。

【図11】同端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャート。

【符号の説明】

10 交換前の携帯電話機

20 メモリーカード

30 交換後の携帯電話機

40 携帯電話通信網

50 ユーザ管理サーバ

100 システムバス

101 CPU

102 RAM

103 ROM

104 外部記憶装置

105 入力装置

106 出力装置

108 携帯電話用通信装置

200 システムバス

201 CPU

202 RAM

203 ROM

204 入力装置

205 出力装置

206 メモリーカードドライブ装置

207 携帯電話用通信装置

501 利用者情報記憶手段

502 暗号鍵情報生成手段

503 暗号鍵情報送信手段

504 端末保存データ受信手段

505 端末保存データ記憶手段

506 端末保存データ送信手段

601 端末保存データ記憶手段

602 暗号鍵情報受信手段

603 暗号鍵情報記憶手段

604 暗号化手段

605 データ書込手段

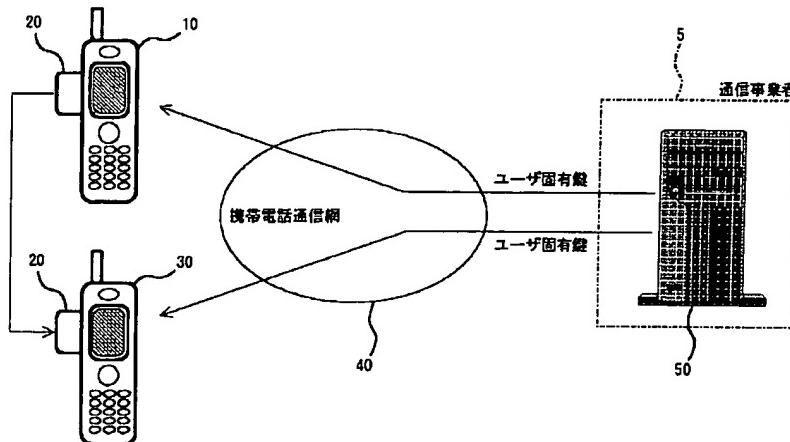
606 データ読込手段

607 復号化手段

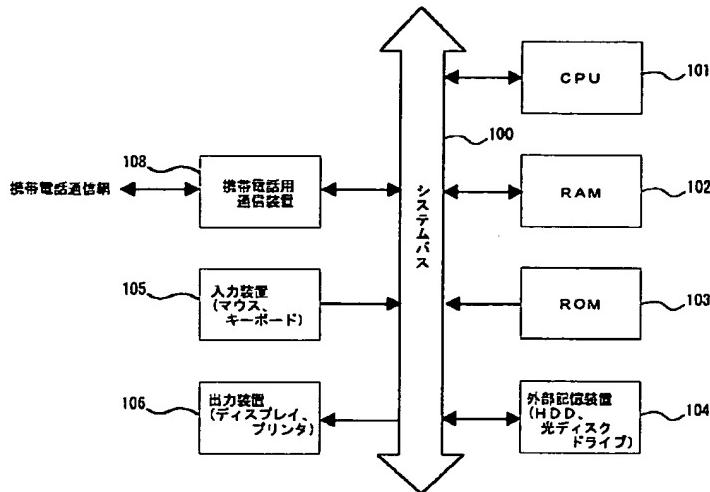
608 端末保存データ送信手段

609 端末保存データ受信手段

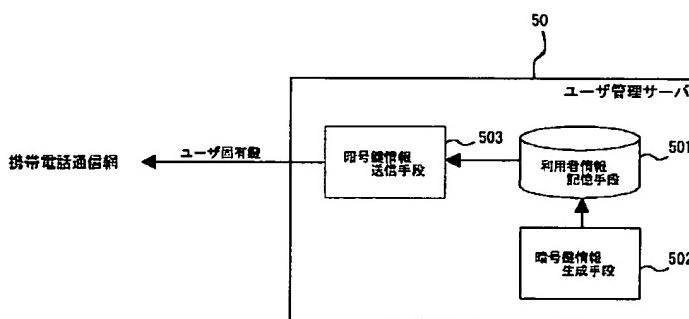
【図1】



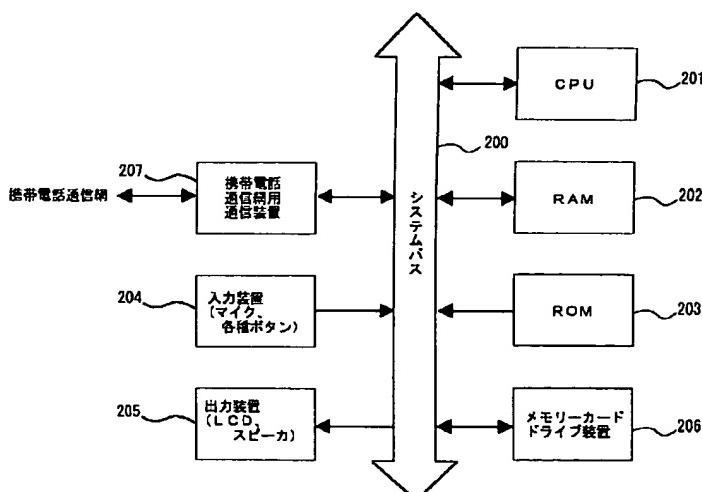
【図2】



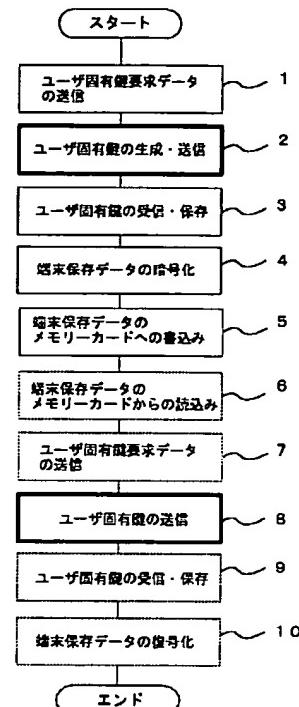
【図3】



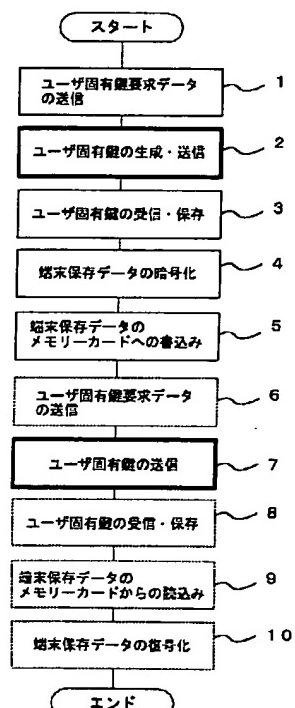
【図4】



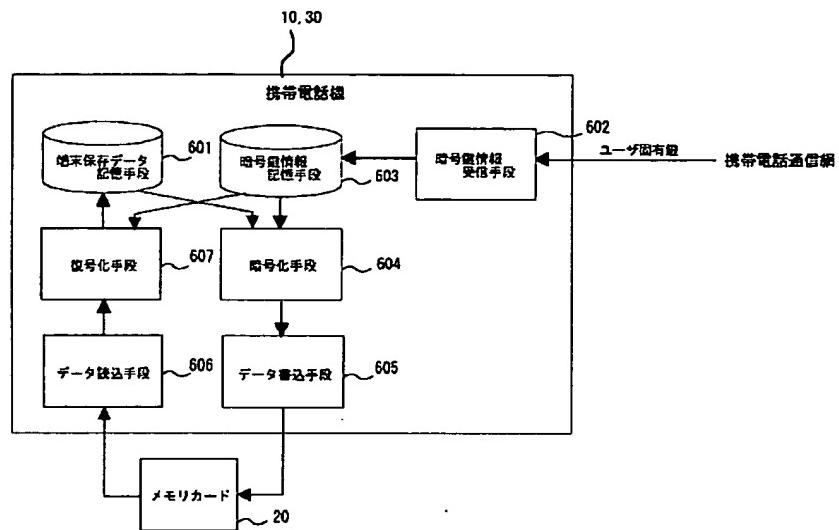
【図6】



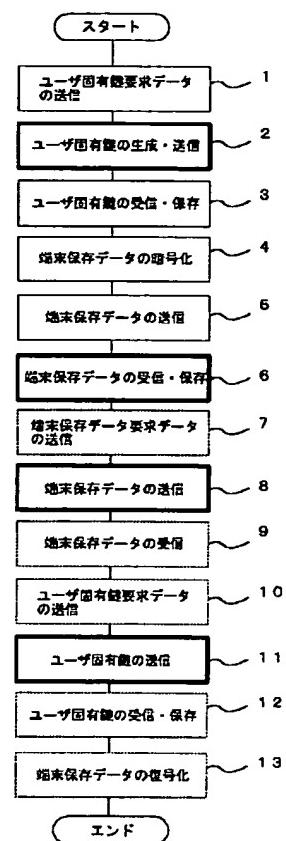
【図7】



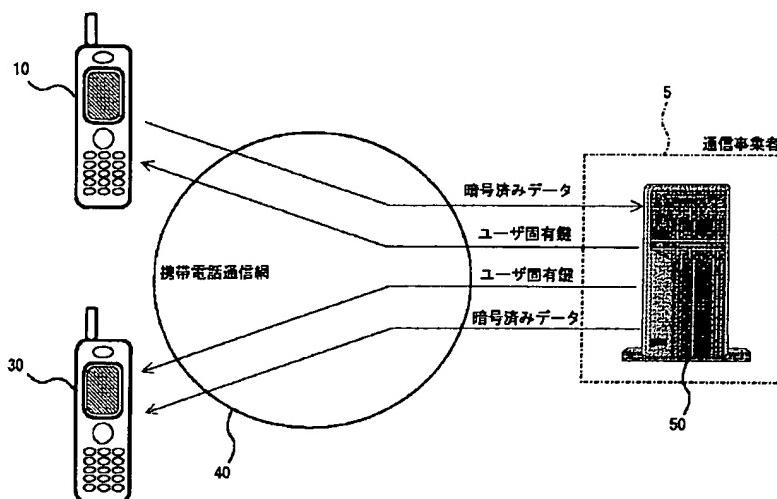
【図5】



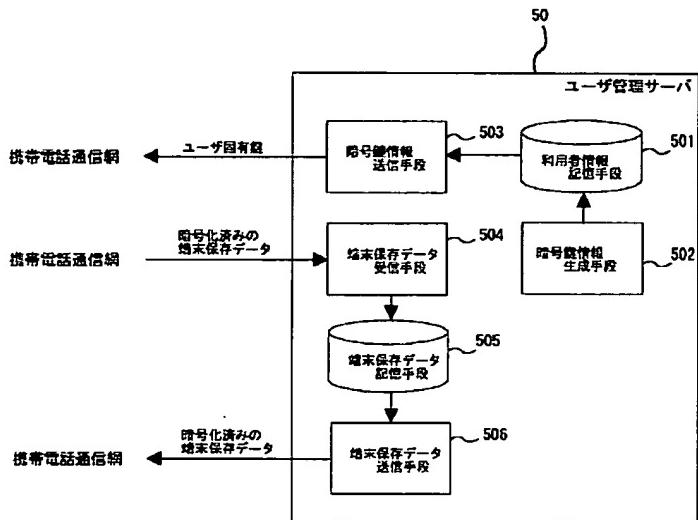
【図11】



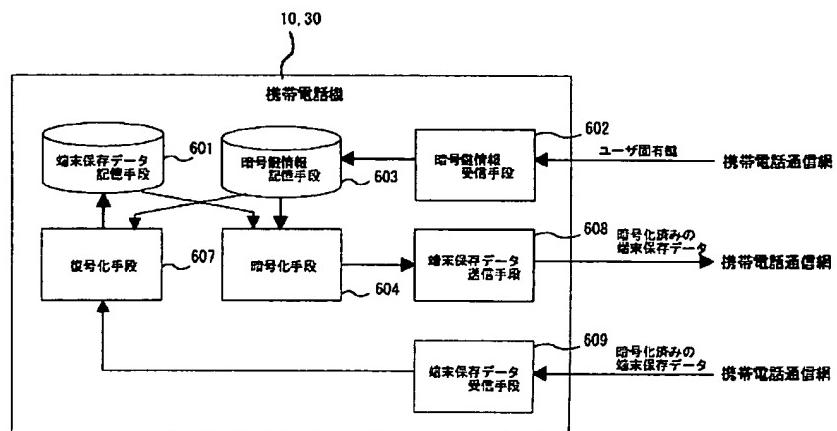
【図8】



【図9】



【図10】



フロントページの続き

(51) Int. Cl. 7

識別記号

H 04 L 9/32

F I

H 04 L 9/00

テマコード (参考)

6 2 1 A

(72) 発明者 深谷 真人

東京都新宿区信濃町34番地 J R 信濃町ビル
ル ジェイフォン東日本株式会社内

F ターム (参考) 5B017 AA03 BA07 CA15 CA16

5B082 GA11 HA05

5J104 AA16 EA04 EA26 NA02 NA27

PA02 PA14